REMARKS:

Claims 1-45 were presented for examination and are pending in this application. In an Official Action dated January 27, 2005, claim 44 was allowed, claim 29 was objected to, and claims 1-28, 30-43, and 45 were rejected. Applicants thank Examiner for examination of the claims pending in this application and addresses Examiner's comments below.

Based on the following Remarks, Applicants respectfully request that Examiner reconsider all outstanding objections and rejections, and withdraw them.

Applicants thank Examiner for indicating the allowance of claim 44 and allowability of claim 29 if re-written in independent form. Applicants further thank Examiner for indicating acceptance of the drawings filed 25 August 2000. Applicants note that an Information Disclosure Statement was filed on January 10, 2005 but have not received Examiner indication that the cited references were considered. Applicants kindly request that that Examiner consider the cited references and provide and indication of his consideration by initialing the filed PTO/SB 08A form.

Claim 4 has been amended to clarify and broaden the scope of the claim commensurate within the scope of protection to which Applicants believe they are entitled. No new matter has been entered.

Response to Claim Rejections based on Hsieh

Claims 1-5, 8-20, 23-28, 30, 33, 34, 39-43, and 45[1] were rejected 35 USC § 102(e) as allegedly being anticipated by Hsieh. This rejection is now traversed.

[1] Applicants note that in p.2 paragraph 5 of the Office Action claim 44 is included ("39-45") in the group of anticipated claims. However, since it is indicated as allowed in the Office Action Summary and in paragraph 12, Applicants presume this to be an oversight and do not address this claim as being rejected.

Independent claims 1, 4, 19, 26, and 30, 33, 34, and 42 each recite a method of examining a network comprising, in relevant part, receiving information from a remote host (or other network equipment) and identifying an operating system and service, or determining vulnerabilities/security policy violations based on information received from the host (or other network equipment) through the network. More specifically, claim 1 identifies an operating system and its patch level and a version and patch level of a service; claim 4 identifies a version of an operating system and a version of a service; claim 19 identifies an operating system and a service; claims 30 and 42 identify a vulnerability; claim 33 infers an unknown vulnerability; and claim 34 identifies a security policy violation.

Advantageously, network-based examination of a host non-intrusively determines host operating system and service conditions. Furthermore, network-based examination is more reliable by inferentially determining network conditions rather than relying on easily compromised (e.g., by hackers) and insufficient (e.g., fail to identify version and/or patch level) self-identification techniques such as banners. Advantageously, by determining a host's conditions to the levels of granularity recited in the claims, down to the version and patch level of an operating system or service, the identification of vulnerabilities, among other things, is more accurate. In particular, vulnerabilities can be addressed in later versions or patches of software, and additional vulnerabilities can result from later versions or patches.

By contrast, Hsieh does not teach or suggest the identification of host conditions, such as operating system ("OS"), service, versions, and patches, based on information received from a remote host through a network, instead it works based on information received from a user. The system described in Hsieh is a "security shield" that prevents

unauthorized access of a system by a user based intercepting the user's requests. See Hsieh, col. 5, lines 27-45. The intercepted user requests are checked based on a rule checking mechanism. After the rule check, the security shield system forwards the requests to the operating system if approved or returns the requests to the user if failed. In the section cited by Examiner, Hsieh clearly describes that its security shield method operates by intercepting requests from the user prior to forwarding them to the operating system:

> Preferably the method comprises means for controlling access to files of the computer system software by redirector means for intercepting a non-interactive command requests, file access requests, program access request, network, and the like, from a computer system user prior to forwarding the request to the operating system software, performing a rule check and a log event function using operating system call interception, returning a failed rule check request to the computer system user via open system call, and forwarding approved requests for continued processing to the operating system. Means for controlling access to interactive programs by redirector means for intercepting an interactive command from a user and returning failed rule check interactive commands to the user and to continue processing succeeded rule check interactive commands are provided. Then, the interactive commands or the non-interactive commands, file access requests, programs, networks, and the like, are forwarded for processing by the operating system software.

Hsieh, col. 5, lines 46-67 (emphasis added). Thus, unlike the claimed invention, Hsieh's method operates on information it receives from users not on information received from the hosts. Accordingly, Hsieh does teach or suggest identifying an operating system and a service from a remote host based on communications with the host through the network.

It should be noted that Hsieh discusses that there are certain known vulnerabilities associated with operating systems, e.g., UNIX and NT "Superuser" access. See, Hsieh, col. 6, lines 49-65. Given that these access-based vulnerabilities exist, Hsieh describes that its security shield method eliminates them by controlling access before a user request is allowed to reach the operating system. However, this does not teach or suggest identifying the

operating system and service of a remote host through network communications from the host.

Accordingly, for at least these reasons, Applicants respectfully submit that claims 1, 4, 19, 26, 30, 33, 34, and 42, and their dependent claims 2, 3, 5-12, 14-18, 20-25, and 27-28 are patentably distinguishable over Hsieh. Therefore, Applicants respectfully request that Examiner reconsider the rejection, and withdraw it.

Further, with respect to dependent claims 6 and 22, the Examiner cites Drake to make up for Hsieh's deficiency in teaching identifying a Trojan application on the host. However, Drake's description is limited to protection of software operating within a single computer system. Hence, the combination of Hsieh and Drake still fail to teach or suggest the claimed identifying operating system and service based on network communications from the host.

Similarly, Hornbuckle is cited with respect to dependent claims 7 and 22 to provide the teaching of identifying unauthorized software use on the host missing in Hsieh. However, Hornbuckle simply describes a software rental system that operates over a network. Hornbuckle does not describe the use of network communications from a host to identify an operating system or service of the host, the claim elements missing in Hsieh. Thus, the combined Hsieh-Hornbuckle reference fails to teach or suggest the claimed identifying operating system and service based on network communications from the host.

Accordingly, for at least these reasons, dependent claims 6, 7, 21, and 22 are patentably distinguishable from the cited references, alone and in combination. Therefore, Applicants respectfully request that Examiner reconsider the rejection, and also withdraw it.

Response to Claim Rejections based on Arnold

Claims 31, 35, 36, and 38 were rejected 35 USC § 102(e) as allegedly being anticipated by Arnold. Claim 35 has been cancelled. Claim 36 is amended herein to expressly incorporate the elements of claim 35, from which it depends. Claims 37 and 38 are amended to reflect their dependency on claim 36. Accordingly, these amendments do not change the scope of these claims. With respect to claims 31, 36, and 38 this rejection is now traversed.

Independent claims 31 and 36 recite identifying a vulnerability (or a Trojan horse) based on a comparison of packet information from packets received from a network. This remote packet based identification of vulnerabilities (or a Trojan horse) beneficially allows to non-intrusively determine network vulnerabilities and to act accordingly without the need to further access the affected network host or other equipment.

By contrast, the method described in Arnold does not identify a vulnerability (or a Trojan horse) from comparing packet data. The virus detection system of Arnold relies on an "anomaly detection" and a subsequent virus scan of the affected system (e.g., files, boot records, memory) to determine whether a virus is present. As shown in FIG. 2, the invention in Arnold first "detects anomalous system behavior of a type that may indicate the presence of an undesirable information state resulting from the presence of a virus or some other undesirable software entity, such as a worm or Trojan Horse." Arnold, col. 4, line 61-66 (emphasis added).

Subsequently, "if preliminary evidence of virus-like activity is detected, additional computational resources are devoted to obtaining more conclusive evidence of viral

infection. ... Thus Step A [sic] scans an informational state history of the system, that is, all relevant media (e.g., files, boot record, memory), for known viruses." Col. 5, lines 29-37.

Thus, the system of Arnold does not identify vulnerabilities (or a Trojan horse) from comparing the packet data, e.g., with a reflex packet database. The system of Arnold, after detecting anomalous system behavior "of a type that may indicate the presence ... of a Trojan Horse," requires a subsequent scan of a system's media resources to identify that indeed a virus is present. Moreover, if the virus is not a known virus, subsequent steps (C-E in FIG. 2) are required to identify the presence of a virus. Thus, the virus-scan of local media within the potentially infected system (e.g., stored executable programs or the like) is what identifies the virus, and not information in the response network packets as recited in the claims.

Accordingly, for at least these reasons, claims 31 and 36 and their dependent claims 37-39 are patentably distinguishable over the Arnold. Therefore, Applicants respectfully request that Examiner reconsider the rejection, and withdraw it.

In addition, with respect to claim 37, the further combination of Hsieh with Arnold still fails to teach or suggest the identification of vulnerabilities based on the comparison of packet information missing in Arnold because Hsieh, as shown above, does not describe using information from the host for identification. Moreover, Hsieh, which the Examiner cites as describing the identification of the host's OS type, version, and patch level and its service type, version, and patch level, does not even teach this. The closest Hsieh gets to describing this OS identification is in it's acknowledgement that certain vulnerabilities are known with respect to certain operating systems, e.g., superuser access in UNIX and NT. However, it does not teach identifying the OS type, version, and the like based on network

communication from the host. Therefore, the combination of Arnold and Hsieh still fails to teach or suggest all the elements of claim 37.

Accordingly, for at least these reasons, claim 37 is patentably distinguishable from the cited references, alone and in combination. Therefore, Applicants respectfully request that Examiner reconsider the rejection, and withdraw it.

Response to Claim Rejections based on Diersch

Claim 32 was rejected 35 USC § 102(e) as allegedly being anticipated by Diersch. Claim 32 is amended herein to correct an oversight in its prior amendment. This rejection is now traversed.

Claim 32 recites a method of examining a network in which based on inferential information in responsive packets from a host unauthorized use of software in the host is identified. The method of claim 32 identifies software that is already in operation at a host system based on the inferential information that such software causes in the responsive packet from the host.

Diersch generally discloses a system for securing protected software against unauthorized use in computer networks. A program blocks further execution of protected programs when failing to establish a connection to an authorization component (Col. 5:24-31). Diersch fails to teach or suggest identifying unauthorized software used in a host based on inferential information in responsive packets from that host. Diersch's system explicitly determines whether a protected program is authorized prior to allowing the program to operate. Because the unauthorized software in Diersch is not allowed to execute, it cannot cause reflex packets from the host to include any particular information from which an inference can be made that identifies that the unauthorized software is being used in the host.

Accordingly, for at least this reason, claim 32 is patentably distinguishable from Diersch. Therefore, Applicants respectfully request that Examiner reconsider the rejection, and withdraw it.

Conclusion

In sum, Applicants respectfully submit that claims 1 through 34 and 36 through 45, as presented herein, are patentably distinguishable over the cited references (including references cited, but not applied). Therefore, Applicants request reconsideration of the basis for the rejections to these claims and request allowance of them.

In addition, Applicants respectfully invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
JOHN S. FLOWERS, ET AL.

Date: April 27, 2005 By: _____

Hector J. Ribera, Attorney of Record
Registration No. 54,397
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7192
Fax: (650) 938-5200
E-Mail: hribera@fenwick.com